

EDWARD J. MARKEY

7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE

RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND
THE INTERNET

SELECT COMMITTEE ON
HOMELAND SECURITY

RESOURCES COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515-2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-2107
(202) 225-2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396-2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875-2900
www.house.gov/markey

February 23, 2004

The Honorable Timothy J. Muris
Chairman, Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

The Honorable Michael K. Powell
Chairman, Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Dear Sirs:

I am writing to express my concern about the applicability and enforcement of U.S. telecommunications, telemarketing and Internet privacy laws and regulations when personal information is out-sourced and sent off-shore by U.S. companies or other persons.

Recent press reports suggest that many U.S. companies are allowing personal data they have collected about American citizens to be transferred to off-shore out-sourcing firms for customer service, analysis, or processing. This off-shoring of personal data appears to be carried out by a wide range of companies – including those in the telemarketing and telecommunications services industries.

I am concerned that potentially sensitive data is increasingly being made available to overseas workers for customer service, transaction processing, or billing purposes, without the knowledge or informed consent of the American public. When personal data is outsourced to companies in India, China, Russia, Vietnam, the Philippines, Malaysia and the Czech Republic or elsewhere, I am concerned about the lack of adequate privacy protection and the potential that such out-sourcing may effectively put abusive conduct beyond the reach of U.S. privacy laws and regulations as well as U.S. law enforcement.

The threat to personal privacy represented by such actions is not merely theoretical. According to press reports, last year a Pakistani woman who had been hired as a subcontractor to perform medical transcription work for a Texas company engaged as an outsourcing firm for a California hospital threatened to post sensitive patient medical records on the Internet unless she received certain payments she claimed were due to her. Press reports indicate that the Pakistani woman

actually posted one file onto the Internet, demonstrating her willingness to carry out her threat if her demands were not met.

This incident highlights the fact that information technology jobs, back office data processing and data analysis jobs, certain financial services sector jobs and some highly technical medical interpretation jobs that used to be performed domestically by Americans, are being out-sourced to off-shore locations by companies seeking to take advantage of the dramatically lower wages available in Third World countries. I am concerned that in their rush to cut costs and increase their bottom line, these companies may be sacrificing or putting in jeopardy the privacy protections the law affords to American citizens by transferring sensitive information to off-shore companies that may be outside of the reach of U.S. privacy law or beyond the jurisdiction of U.S. regulators.

I therefore request that you explain what steps are being undertaken by your agency to protect the privacy of personal information collected about American citizens by companies or other persons subject to your oversight and supervision. In addition, I specifically request your assistance and cooperation in providing responses to the following questions:

Questions for FTC

- 1) The Child Online Privacy Protection Act (15 U.S.C. 6501-6506) contains certain prohibitions on the use of websites to collect personal information from children 12 and under. In particular, such websites must obtain parental permission prior to collecting such information and the FTC has developed rules to ensure that adequate parental notice and verifiable permission are attained to protect children.
 - A) To the extent that entities operate websites and also utilize off-shore companies for customer service or billing operations, do the Commission's rules prohibit the collection and disclosure under COPPA of information gathered from children to entities operating off-shore?
 - B) Do the Commission's rules implementing COPPA address issues of enforcement for websites operating outside the United States?
 - C) What action has the Commission taken to address such off-shore consumer protection issues generally, and with COPPA specifically, with respect to off-shore enforcement?
- 2) Do-Not-Call – The recently implemented “Do-Not-Call” database permits consumers to protect themselves from unwanted telemarketing calls. As you well know, tens of millions of phone numbers have been registered in the database since it began.
 - A) Is the Commission aware of telecommunications carriers or other entities within the Commission's jurisdiction moving their telemarketing operations off-shore?
 - B) Does the Commission have sufficient authority to enforce violations of the Do-Not-Call rules by foreign telemarketing entities operating off-shore? Does the Commission have sufficient authority to enforce the Do-Not-Call rules on telemarketing entities operating off-shore if such entities are performing such telemarketing on behalf of a U.S.-domiciled company or entity?
 - C) Has the Commission initiated or succeeded in bringing any enforcement action against off-shore telemarketing operations in violation of the Commission's rules in the last 3 years?

Questions For FCC

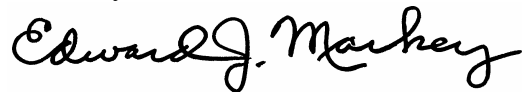
1) Section 222 of the Communications Act of 1934 (47 U.S.C. 222) contains privacy protections for consumers with respect to “customer proprietary network information,” or CPNI. As you know, CPNI is the personal information related to a consumer’s use of telecommunications services, including the information contained in bills for such services as well as the type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier. In general, telecommunications carriers may only “use, disclose, or permit access to individually identifiable” CPNI with the “approval of the customer.” While Section 222 does include some important exceptions to these protections, including for purposes of rendering and billing for service, I am concerned about risks to consumer privacy in cases where a carrier shifts customer service or billing operations offshore. In particular I am eager to get the answers to the following questions regarding the Commission’s implementation and enforcement of Section 222:

- A) Do the Commission’s rules implementing Section 222 permit the disclosure of CPNI by a telecommunications carrier to entities or persons operating in territories outside of the United States?
 - B) If so, what enforcement limitations may result for the Commission if CPNI data is permitted to be disclosed to entities operating overseas if violations to CPNI occur as a result of impermissible disclosures by that offshore entity?
- 2) Section 631 of the Communications Act of 1934 (47 U.S.C. 551) contains privacy protections for consumers with respect to “any wire or radio communications service” offered by a cable operator. This consists of cable service, as well as broadband access to the Internet or other telecommunications services to the extent to which cable facilities are used to provide that service.
- A) Is the Commission aware of practices in the cable industry that involve moving customer service support or billing operations overseas?
 - B) Does the Commission believe disclosures of personal information in violation of Section 631 in cases where violations occur off-shore thwarts or unduly hampers enforcement remedies contained in Section 631?
- 3) Do-Not-Call – The recently implemented “Do-Not-Call” database permits consumers to protect themselves from unwanted telemarketing calls. Tens of millions of phone numbers have been registered in the database since it began.
- A) Is the Commission aware of telecommunications carriers or other entities within the Commission’s jurisdiction moving their telemarketing operations off-shore?
 - B) Does the Commission have sufficient authority to enforce violations of the Do-Not-Call rules by foreign telemarketing entities operating off-shore? Does the Commission have sufficient authority to enforce the Do-Not-Call rules on telemarketing entities operating off-shore if such entities are performing such telemarketing on behalf of a U.S.-domiciled company or entity?
 - C) Has the Commission initiated or succeeded in bringing any enforcement action against off-shore telemarketing operations in violation of the Commission’s rules in the last 3 years?

D) Does the Commission have sufficient authority to enforce provisions of Section 227 of the Communications Act of 1934 (47 U.S.C. 227) governing the use of facsimile machines, computers, or other devices for transmitting unsolicited “junk faxes” if such transmissions originate off-shore? Has the Commission successfully enforced such provisions against the off-shore origination of junk faxes in the past? How many complaints has the Commission received in the last 3 years with respect to unsolicited facsimiles?

Thank you for your assistance in providing responses to these questions. If you have any questions about this inquiry, please feel free to have your staff contact Dr. Michael Bailey or Colin Crowell of my staff at 202-225-2836.

Sincerely,

A handwritten signature in black ink that reads "Edward J. Markey". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Edward J. Markey
Member of Congress